PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 16.08.2001

E T U O I K E U S T O D I S T U S
P R I O R I T Y D O C U M E N T

Hakija
Applicant

1. **Sonera Smarttrust Oy, Helsinki, FI**
2. **Vatanen, Harri, Englefield Green, GB**
3. **Liukkonen, Jukka, Helsinki, FI**
4. **Hiltunen, Matti, Helsinki, FI**

Kansainvälinen patenttihakemus nro
International patent application no **PCT/FI00/00116**

Kansainvälinen tekemispäivä
International filing date **16.02.2000**

Etuoikeushak. nro
Priority from appl. **FI 990323**

Tekemispäivä
Filing date **16.02.1999**

Keksinnön nimitys
Title of invention

"Method for the provision of data security"

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä kansainvälisiä patenttihakemuksia vastaanottavana viranomaisena toimivalle Patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista sekä niihin tehdyistä korjauksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawing, originally filed with the Finnish Patent Office acting as receiving Office for the international patent applications, and of any corrections thereto.

Pirjo Kaila
Tutkimussihteeri

Maksu 300,- mk
Fee 300,- FIM

Osoite: Arkadiankatu 6 A
Address: P.O.Box 1160
FIN-00101 Helsinki, FINLAND
Puhelin: 09 6939 500
Telephone: + 358 9 6939 500
Telefax: 09 6939 5204
Telefax: + 358 9 6939 5204

HOME COPY

PCT REQUEST

12869S

Original (for SUBMISSION) - printed on 16.02.2000 03:15:09 PM

0 0-1	For receiving Office use only International Application No.	PCT/FI00/00116
0-2	International Filing Date	(16-02-2000) 16 FEB 2000
0-3	Name of receiving Office and "PCT International Application"	The Finnish Patent Office PCT International Application
0-4 0-4-1	Form - PCT/RO/101 PCT Request Prepared using	PCT-EASY Version 2.90 (updated 15.12.1999)
0-5	Petition The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	Receiving Office (specified by the applicant)	National Board of Patents and Registration (Finland) (RO/FI)
0-7	Applicant's or agent's file reference	12869S
I	Title of Invention	METHOD FOR THE PROVISION OF DATA SECURITY
II II-1 II-2 II-4 II-5 II-6 II-7	Applicant This person is: Applicant for Name Address: State of nationality State of residence	 applicant only all designated States except US SONERA SMARTTRUST OY c/o Sonera Oyj P.O. Box 106 FIN-00051 SONERA Finland FI FI
III-1 III-1-1 III-1-2 III-1-4 III-1-5 III-1-6 III-1-7	Applicant and/or inventor This person is: Applicant for Name (LAST, First) Address: State of nationality State of residence	 applicant and inventor US only VATANEN, Harri 2 Rushmere Place Englefield Green, Surrey TW20 0NN United Kingdom FI GB

PCT REQUEST

12869S

Original (for SUBMISSION) - printed on 16.02.2000 03:15:09 PM

III-2	Applicant and/or inventor	
III-2-1	This person is:	applicant and inventor
III-2-2	Applicant for	US only
III-2-4	Name (LAST, First)	LIUKKONEN, Jukka
III-2-5	Address:	Männikkötie 9 G 53 FIN-00630 Helsinki Finland
III-2-6	State of nationality	FI
III-2-7	State of residence	FI
III-3	Applicant and/or inventor	
III-3-1	This person is:	applicant and inventor
III-3-2	Applicant for	US only
III-3-4	Name (LAST, First)	HILTUNEN, Matti
III-3-5	Address:	Kaarlenkatu 10 B 59 FIN-00530 Helsinki Finland
III-3-6	State of nationality	FI
III-3-7	State of residence	FI
IV-1	Agent or common representative; or address for correspondence The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	agent
IV-1-1	Name	PAPULA REIN LAHTELA OY
IV-1-2	Address:	P.O. Box 981 (Fredrikinkatu 61 A) FIN-00101 HELSINKI Finland
IV-1-3	Telephone No.	+358 9 3480 060
IV-1-4	Facsimile No.	+358 9 3480 0630
IV-1-5	e-mail	papula@papula.fi
V	Designation of States	
V-1	Regional Patent (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	AP: GH GM KE LS MW SD SL SZ TZ UG ZW and any other State which is a Contracting State of the Harare Protocol and of the PCT EA: AM AZ BY KG KZ MD RU TJ TM and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE and any other State which is a Contracting State of the European Patent Convention and of the PCT OA: BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG and any other State which is a member State of OAPI and a Contracting State of the PCT

PCT REQUEST

12869S

Original (for SUBMISSION) - printed on 16.02.2000 03:15:09 PM

V-2	National Patent (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	AE AL AM AT AU AZ BA BB BG BR BY CA CH&LI CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
V-5	**Precautionary Designation Statement** In addition to the designations made under items V-1, V-2 and V-3, the applicant also makes under Rule 4.9(b) all designations which would be permitted under the PCT except any designation(s) of the State(s) indicated under item V-6 below. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit.	
V-6	**Exclusion(s) from precautionary designations**	NONE
VI-1	**Priority claim of earlier national application**	
VI-1-1	Filing date	16 February 1999 (16.02.1999)
VI-1-2	Number	990323
VI-1-3	Country	FI
VII-1	**International Searching Authority Chosen**	Swedish Patent Office (ISA/SE)

		number of sheets	electronic file(s) attached
VIII	**Check list**		
VIII-1	Request	4	-
VIII-2	Description	5	-
VIII-3	Claims	2	-
VIII-4	Abstract	1	12869s.txt
VIII-5	Drawings	2	-
VIII-7	TOTAL	14	
	Accompanying items	paper document(s) attached	electronic file(s) attached
VIII-8	Fee calculation sheet	✓	-
VIII-9	Separate signed power of attorney	✓	-
VIII-9	Separate signed power of attorney	✓	-
VIII-10	Copy of general power of attorney	✓	-
VIII-12	Priority document(s)	Item(s) VI-1	-
VIII-16	PCT-EASY diskette	-	diskette
VIII-17	Other (specified):	copy of official action / FI 990323	-
VIII-18	**Figure of the drawings which should accompany the abstract**	1	
VIII-19	**Language of filing of the international application**	Finnish	

PCT REQUEST 12869S

Original (for SUBMISSION) - printed on 16.02.2000 03:15:09 PM

IX-1	Signature of applicant or agent	
IX-1-1	Name	PAPULA REIN LAHTELA OY
IX-1-2	Name of signatory	Markku Simmelvuo

FOR RECEIVING OFFICE USE ONLY

10-1	Date of actual receipt of the purported international application	(16 -02- 2000) 16 FEB 2000
10-2	Drawings:	
10-2-1	Received	
10-2-2	Not received	
10-3	Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application	
10-4	Date of timely receipt of the required corrections under PCT Article 11(2)	
10-5	International Searching Authority	ISA/SE
10-6	Transmittal of search copy delayed until search fee is paid	

FOR INTERNATIONAL BUREAU USE ONLY

11-1	Date of receipt of the record copy by the International Bureau	

MENETELMÄ TIEDON TURVAAMISEKSI

KEKSINNÖN ALA

Esillä oleva keksintö liittyy tietoliikennejärjestelmiin. Erityisesti keksintö liittyy uudentyyppiseen menetelmään, jonka avulla sanoma välitetään vastaanottajalle allekirjoitettuna ja/tai salattuna. Samalla varmistutaan sanoman lähettäjän henkilöllisyydestä ja sanoman sisällön oikeellisuudesta.

TEKNIIKAN TASO

Tiedon siirtäminen paikasta toiseen bittivirtana on helppoa. Sen sijaan vaikeampaa on varmistua siitä, että siirretty tieto säilyy siirron aikana muuttumattomana. Vastaavasti yhä useammassa tiedonsiirtotapauksessa halutaan varmistua myös siitä, että siirrettävä tieto päätyy hyödyllisenä vain sille osapuolelle, jolle tieto alun perin on tarkoitettu. Tämän tarkoitusperän saavuttamiseksi käytetään salausta. Salauksen avulla pyritään siis varmistamaan se, että tieto on hyödyllistä vain sille, jolla on salauksen purkuun oikeuttava purkuavain. Salauksen vahvuus perustuu siihen, että tietokoneet eivät pysty murtamaan salausta äärellisessä ajassa.

Sanomista puhuttaessa viitataan ensisijaisesti matkaviestinjärjestelmien, edullisesti GSM-järjestelmän (GSM, Global System for Mobile communications), lyhytsanomiin (SMS, Short Message Service). Sanoma voi kuitenkin tarkoittaa myös minkä tahansa muun tietoliikennejärjestelmän sanomatyyppiä.

Matkaviestinjärjestelmän, edullisesti GSM-järjestelmän, mukaisia lyhytsanomia on mahdollista salata, jotta pystytään estämään sanoman näkyminen selväkielisenä ulkopuolisille osapuolille. Lyhytsanoma salataan ja sanomasta muodostetaan lisäksi tarkisteosa esimerkiksi hash-funktioilla. Tarkisteosa ja salattu sanoma lähetetään erikseen lyhytsanomina vastaanotta-

jalle. Vastaanottaja purkaa sanoman ja toisessa sanomassa tullutta tarkisteosaa verrataan purettuun tieto-osaan.

Edellä mainitussa ratkaisussa on ongelmana se, että koko toimenpide, sanoman allekirjoitus, salaaminen ja tarkisteosan generointi täytyy välittää vastaanottajalle kahdessa erillisessä sanomassa, edullisesti lyhytsanomassa.

Keksinnön tarkoituksena on poistaa edellä mainitut epäkohdat tai ainakin merkittävästi lieventää niitä.

Erityisesti keksinnön tarkoituksena on tuoda esiin uudentyyppinen menetelmä, jonka avulla sanoman salaus ja/tai allekirjoitus ja sanoman lähettäjän sekä sanoman sisällön oikeellisuuden varmentaminen on mahdollista tehdä yhden lyhytsanoman välityksellä. Haluttu salattu sanoma ja lähettäjän sekä vastaanottavan osapuolen yksikäsitteinen varmennustieto välitetään yhdessä normaalissa sanomassa, edullisesti GSM-järjestelmän lyhytsanomassa.

Esillä olevan keksinnön tunnusomaisten seikkojen osalta viitataan patenttivaatimuksiin.

KEKSINNÖN YHTEENVETO

Keksinnön mukainen menetelmä koskee sanoman salaamista ja/tai allekirjoittamista sekä sanoman lähettäjän ja sanoman sisällön oikeellisuuden varmentamista. Menetelmässä sanoma erotetaan kahdeksi tai useammaksi osaksi, joihin osiin kuuluu ainakin otsikko-osa ja varsinainen tieto-osa. Otsikko-osa sisältää tietoa sanoman lähettäjästä eli siitä, kuka sanoman allekirjoittaja on. Salaisen ja julkisen avaimen salausmenetelmässä otsikko-osassa on tieto siitä, kenen julkisella allekirjoitusavaimella allekirjoitus voidaan purkaa.

Sanoman sisällön oikeellisuuden varmentamiseksi sanoman tieto-osan sisällöstä muodostetaan tar-

kistusosa, joka liitetään tieto-osan loppuun. Tarkistusosa voidaan muodostaa tarkoitukseen sopivalla hash-funktiolla. Sanoman oikeellisuuden todentaminen perustuu siihen, että sekä lähettäjä että vastaanottaja käyttävät samaa hash-funktiota. Jos salausta yritetään purkaa väärällä avaimella, tarkistusosat poikkeavat toisistaan. Samalla tarkistusosa toimii tarkistussummana, joka ilmaisee mahdollisesti tapahtuneet siirtovirheet. Kun tarkistusosa on liitetty tieto-osan perään, sanoma salataan. Salausmenetelmänä voidaan käyttää julkisen ja salaisen avaimen menetelmää, joka tuottaa vahvan salauksen. Salausalgoritmina voi olla esimerkiksi RSA-algoritmi (RSA, Rivest, Shamir, Adleman) tai muu vahvan salauksen tuottava menetelmä.

Sanoman vastaanottaja pystyy päättelemään käytetyn salausmenetelmän sanoman otsikko-osaan liitetystä tunnisteesta. Jos käytetään julkisen ja salaisen avaimen menetelmää, sanoman tieto-osa ensin allekirjoitetaan lähettäjän salaisella allekirjoitusavaimella. Purkuvaiheessa vastaanottaja varmistuu yksikäsitteisesti lähettäjän henkilöllisyydestä, kun sanoma puretaan lähettäjän julkisella avaimella. Allekirjoituksen jälkeen sanoma vielä salataan, esimerkiksi vastaanottajan julkisella allekirjoitusavaimella. Täten purkuvaiheessa vain oikea vastaanottaja omalla salaisella avaimella pystyy purkamaan salatun sanoman selväkieliseksi.

Jos huomataan, että sanoman sisältö poikkeaa odotetusta, voidaan vaatia sanoman uudelleenlähetystä. Menetelmä voidaan varustaa myös sellaisella toiminnolla, että sanoman lähettäjälle lähetetään kuittaus sanoman onnistuneesta lähetyksestä.

Edellä sanoman salausta ja allekirjoitusta on selitetty GSM-järjestelmän avulla. GSM-järjestelmässä toimien sanoman salaus ja/tai allekirjoitus voidaan tehdä matkaviestimellä. GSM-järjestelmä on kuitenkin

vain yksi edullinen esimerkki käytettävästä järjestelmästä.

Esillä olevan keksinnön etuna tunnettuun tekniikkaan on, että sanoman allekirjoitus ja/tai salaus sekä lähettäjän ja sanoman sisällön oikeellisuuden varmentaminen voidaan välittää yhdessä sanomassa, esimerkiksi GSM-järjestelmän mukaisessa lyhytsanomassa. Lisäksi etuna on, että sanoman allekirjoittajan avain voidaan identifioida vain viidellä tavulla.

KUVALUETTELO

Seuraavassa keksintöä selostetaan yksityiskohtaisesti sovellusesimerkkien avulla, jossa

kuva 1 esittää erästä edullista esillä olevan keksinnön mukaista menetelmää, ja

kuva 2 esittää kuvan 1 mukaisen menetelmän otsikko-osan tunnisteen muodostamista.

Kuvassa 1 esitetään allekirjoitetun ja salatun SMS-sanoman rakenne. Tässä esimerkissä käytetään julkisen ja salaisen avaimen menetelmää ja RSA-algoritmia. Sanoman otsikko-osassa 1 on keksinnön mukaisesti lähettäjän 1. allekirjoittajan tunniste MUI (MUI, Mobile User Identification). Otsikko-osan pituus on 12 tavua eli 96 bittiä. Tieto-osan 2 loppuun on lisätty MD_5-tarkistusosa, joka on pituudeltaan 16 tavua. Tarkistusosa muodostetaan tieto-osan 2 sisällön perusteella hash-funktiolla, joka tässä esimerkissä on MD5 (MD, Message Digest). Seuraavassa vaiheessa tieto-osa 2 allekirjoitetaan lähettäjän salaisella allekirjoitusavaimella. Tuloksena syntyy lähettäjän allekirjoittama tieto-osa 4. Otsikko-osan 3 MUI(PidKey)-kenttään on nyt liitettynä sanoman allekirjoittajan tunniste. Lähettäjän tunniste MUI(PidKey) on viisi tavua pitkä kenttä. Tunniste ilmaisee sen, kenen julkisella allekirjoitusavaimella allekirjoitus voidaan purkaa ja todentaa. Julkinen avain voi olla etukäteen

vastaanottajan tiedossa tai se voidaan kysyä TTP:ltä (TTP, Trusted Third Party).

Seuraavassa vaiheessa otsikko-osa 3 pysyy muuttumattomana. Tieto-osa 4 sen sijaan salataan vielä vastaanottajan julkisella avaimella. Tuloksena syntyy tieto-osa 6, joka on sekä allekirjoitettu että salattu. Edellä mainittujen toimenpiteiden avulla lähettäjän sekä tieto-osan sisällön oikeellisuudesta pystytään varmistumaan. Sanoman kokonaispituus on GSM-järjestelmän lyhytsanomaviestin mukaisesti 140 tavua (160 merkkiä).

Kuvassa 2 esitetään kuvassa 1 esitetyn sanoman otsikko-osan MUI(PidKey)-tunnisteen muodostus. Luotavaan tunnisteosaan liitetään tietty nimi (lohko 21). Nimen, lähettäjän julkisen allekirjoitusavaimen (pituus n. 160bit) ja 1024 bittiä pitkästä jakojäännöksestä (lohko 22) muodostamasta kokonaisuudesta tehdään hash-funktiolla tiivistetty tunniste. Käytettävä hash-funktio voi olla esimerkiksi SHA1 (SHA, Secure Hashing Algorithm) tai MD5. Tiivistyksen seurauksena syntyy 20 tavua pitkä kenttä (lohko 23). MUI(PidKey)-tunniste (lohko 24) muodostetaan ottamalla viisi viimeistä tavua hash-funktiolla tiivistetystä tunnisteesta.

Keksintöä ei rajata pelkästään edellä esitettyjä sovellusesimerkkejä koskevaksi, vaan monet muunnokset ovat mahdollisia pysyttäessä patenttivaatimusten määrittelemän keksinnöllisen ajatuksen puitteissa.

PATENTTIVAATIMUKSET

1. Menetelmä sanoman allekirjoittamiseksi ja/tai salaamiseksi ja sanoman lähettäjän sekä sanoman sisällön oikeellisuuden varmentamiseksi, jossa menetelmässä sanoma erotetaan kahdeksi tai useammaksi osaksi, joihin osiin kuuluu ainakin otsikko-osa ja varsinainen tieto-osa, jossa menetelmässä muodostetaan sanoma ja lähetetään se salattuna ennalta määritetylle vastaanottajalle, t u n n e t t u siitä, että menetelmään kuuluu vaiheet:

muodostetaan tieto-osan sisällöstä tarkistusosa, joka liitetään tieto-osan loppuun;

liitetään sanoman otsikko-osaan lähettäjän tunniste; ja

salataan ja/tai allekirjoitetaan sanoman tieto-osa salausmenetelmällä, jonka avulla sanoman vastaanottaja ja lähettäjä voidaan varmuudella yksilöidä.

2. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että muodostetaan sanoman tieto-osan loppuun liitettävä tarkistusosa hash-funktiolla.

3. Patenttivaatimusten 1 ja 2 mukainen menetelmä, t u n n e t t u siitä, että käytetään sanoman allekirjoitukseen ja/tai salaukseen julkisen ja salaisen avaimen menetelmää.

4. Patenttivaatimusten 1 - 3 mukainen menetelmä, t u n n e t t u siitä, että käytettävä salausalgoritmi on RSA-algoritmi tai vastaava vahvan salauksen tuottava algoritmi.

5. Patenttivaatimusten 1 - 4 mukainen menetelmä, t u n n e t t u siitä, että päätellään käytetty salausmenetelmä sanoman otsikko-osaan liitetystä tunnisteesta.

6. Patenttivaatimuksen 1 - 5 mukainen menetelmä, t u n n e t t u siitä, että liitetään sanoman otsikko-osaan lähettäjän tunniste, joka ilmaisee vastaanottajalle, kenen julkisella allekirjoitusavaimella allekirjoitus puretaan ja todennetaan.

7. Patenttivaatimusten 1 - 6 mukainen menetelmä, t u n n e t t u siitä, että allekirjoitetaan sanoman tieto-osa digitaalisella allekirjoituksella.

8. Patenttivaatimusten 1 - 7 mukainen menetelmä, t u n n e t t u siitä, että allekirjoitetaan sanoman tieto-osa lähettäjän salaisella allekirjoitusavaimella.

9. Patenttivaatimusten 1 - 8 mukainen menetelmä, t u n n e t t u siitä, että salataan lähettäjän julkisella allekirjoitusavaimella salattu sanoman tieto-osa vastaanottajan julkisella salausavaimella.

10. Patenttivaatimusten 1 - 9 mukainen menetelmä, t u n n e t t u siitä, että puretaan vastaanotettu sanoma vastaanottajan salaisella avaimella.

11. Patenttivaatimuksen 1 - 10 mukainen menetelmä, t u n n e t t u siitä, että varmistutaan sanoman lähettäjästä purkamalla vastaanotettu sanoma uudestaan lähettäjän julkisella allekirjoitusavaimella.

12. Patenttivaatimusten 1 - 11 mukainen menetelmä, t u n n e t t u siitä, että varmistutaan puretun sanoman oikeellisuudesta sanoman tieto-osan tarkiste-osan perusteella.

13. Patenttivaatimusten 1 - 12 mukainen menetelmä, t u n n e t t u siitä, että pyydetään sanoman uudelleenlähetystä, jos sanoman sisältö havaitaan virheelliseksi.

14. Patenttivaatimusten 1 - 13 mukainen menetelmä, t u n n e t t u siitä, että vastaanotetaan kuittaus sanoman onnistuneesta lähettämisestä.

15. Patenttivaatimusten 1 - 14 mukainen menetelmä, t u n n e t t u siitä, että käytetään sanoman salausta ja lähettäjän sekä sanoman sisällön varmentamista matkaviestinjärjestelmässä, esimerkiksi GSM-järjestelmässä.

16. Patenttivaatimusten 1 - 15 mukainen menetelmä, t u n n e t t u siitä, että allekirjoitetaan ja/tai salataan sanoma matkaviestimellä.

(57) TIIVISTELMÄ

Esillä olevan keksinnön mukaisen menetelmän tarkoituksena on mahdollistaa se, että sanoma välitetään vastaanottajalle allekirjoitettuna ja/tai salattuna sekä se, että sanomasta voidaan varmuudella varmistaa sanoman lähettäjän henkilöllisyys ja sisällön oikeellisuus. Menetelmässä sanoma jaetaan kahteen tai useampaan osaan. Ensimmäisen osaan, otsikko-osaan, liitetään lähettäjän tunniste. Toisen osan, tieto-osan, loppuun liitetään tieto-osan sisällöstä muodostettu tarkistusosa. Lopuksi sanoman tieto-osa allekirjoitetaan ja/tai salataan siten, että sanoman lähettäjä ja vastaanottaja voidaan varmuudella yksilöidä. Tarkistusosan perusteella voidaan varmentaa sisällön oikeellisuus sekä se, että sanoma on purettu oikeilla avaimilla.

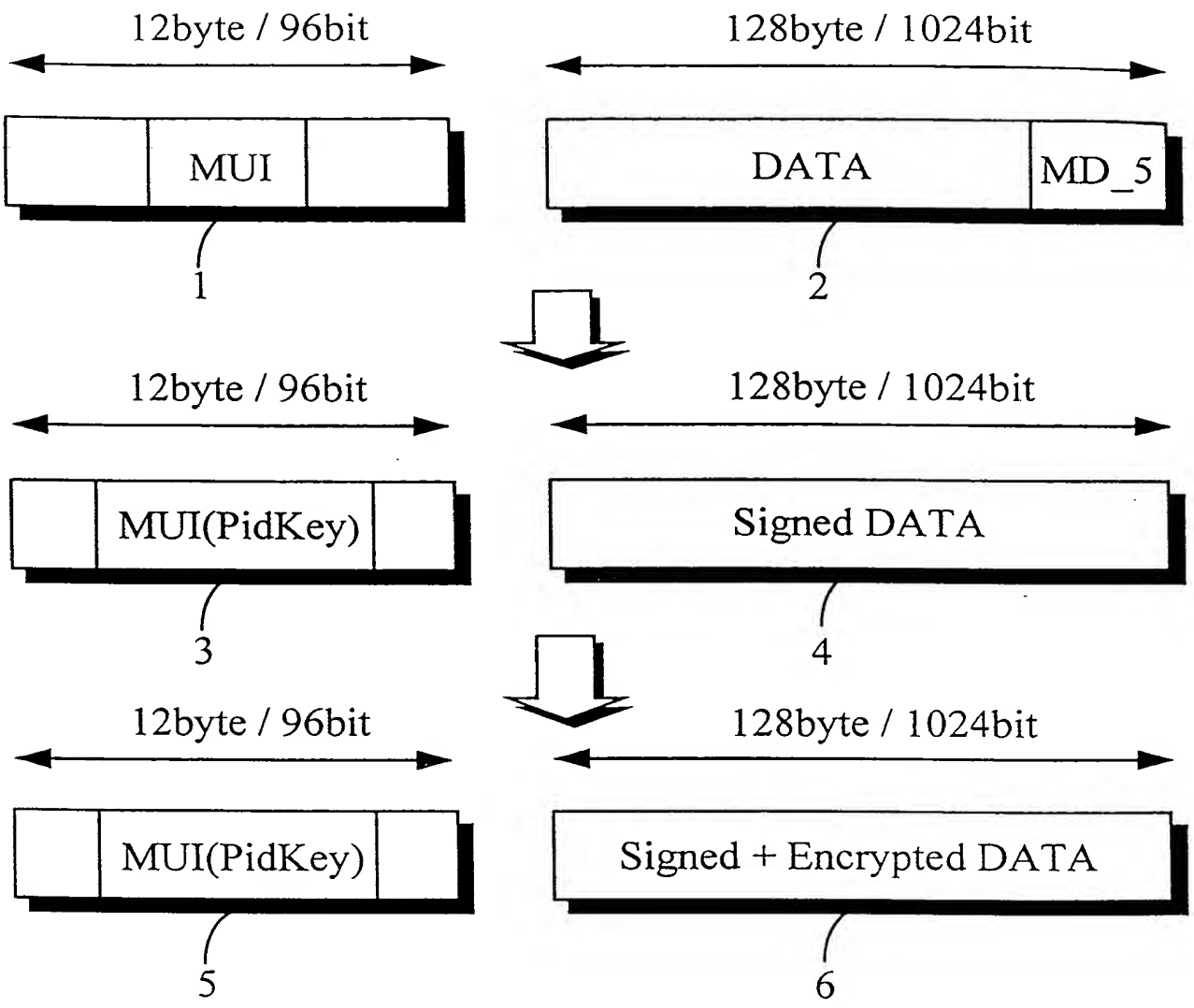
12byte / 96bit
128byte / 1024bit
MUI
DATA
MD_5
1
2
12byte / 96bit
128byte / 1024bit
MUI(PidKey)
Signed DATA
3
4
12byte / 96bit
128byte / 1024bit
MUI(PidKey)
Signed + Encrypted DATA
5
6

Fig. 1

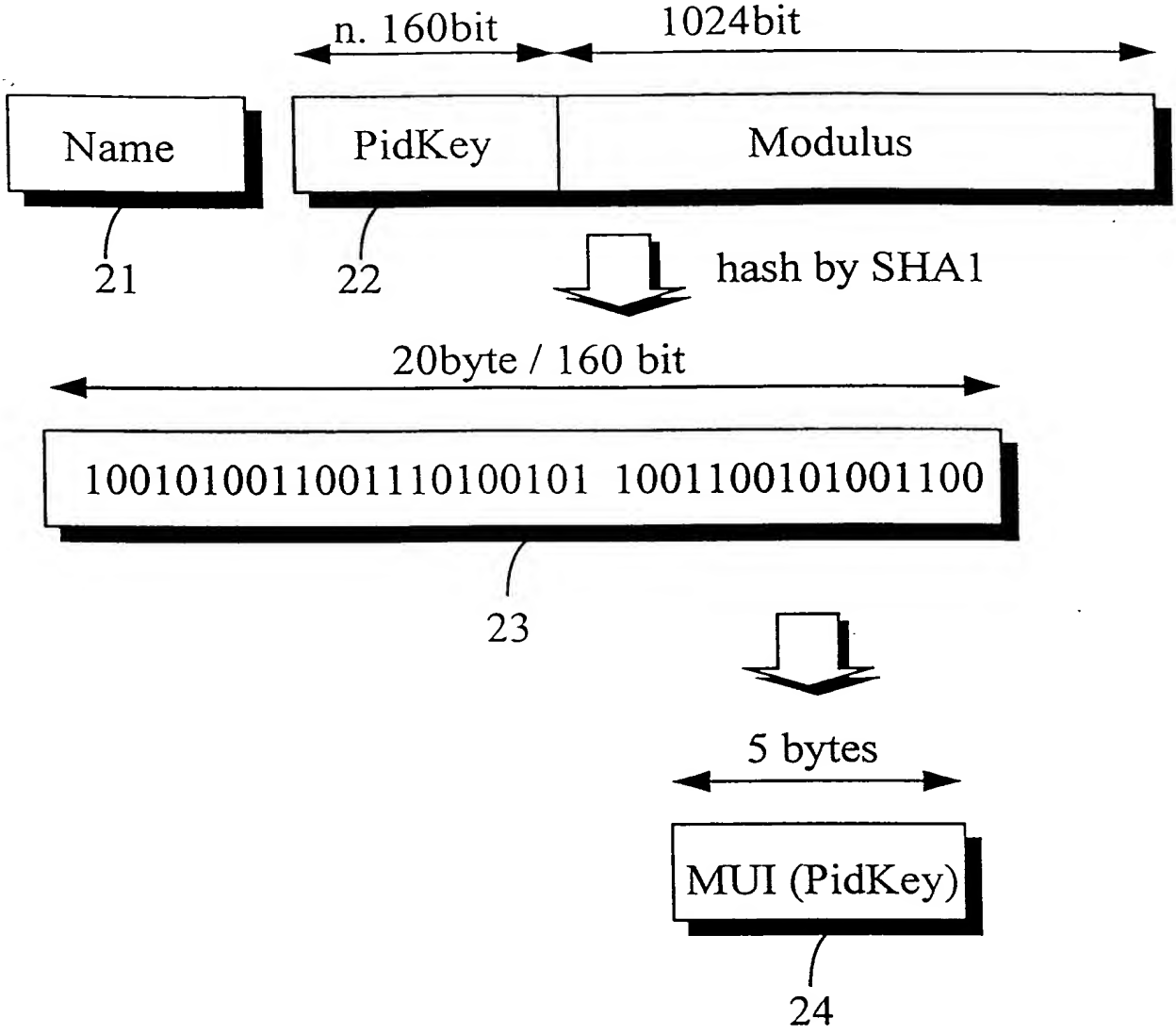
n. 160bit
1024bit
Name
PidKey
Modulus
21
22
hash by SHA1
20byte / 160 bit
10010100110011110100101 10011001010011100
23
5 bytes
MUI (PidKey)
24

Fig. 2